a3 cont

performed on the results produced in step 188. Once again, "l" is the number of bits composing the output string or message. In step 192 the shortened message or string of "l" bits is outputted. It should be noted that the process of FIG. 3 reduced "k" messages of "n" bits each to one message of "l" bits. It should also be noted that the hashing method of FIG. 3 is a $\varepsilon\Delta$ universal hashing method that satisfies the properties of Equations (1) and (2).

IN THE CLAIMS

Amended claims 1-3

1. A method for producing a shortened representation of a collection of bits, comprising the steps of:

inputting the collection of "n" bits;

summing a key having at least "n" bits with the collection of bits to produce a sum;

squaring the sum to produce a squared sum;

performing a modular "p" operation on the squared sum, where "p" is a first prime number greater than 2^n to produce a modular "p" result;

a4

performing a modular 2^l operation on the modular "p" result to produce a modular 2^l result where, "l" is less than "n"; and

outputting the modular 2^l result.

2. A method for producing a shortened representation of a collection of bits, comprising the steps of:

inputting the collection of "n" bits;

summing a first key having at least "n" bits with the collection of bits to produce a first sum;

squaring the first sum to produce a squared sum;

summing the squared sum with a second key having at least "n" bits to produce a second sum;

performing a modular "p" operation on the second sum, where "p" is a first prime number greater than 2^n to produce a modular "p" result;

performing a modular 2^l operation on the modular "p" result to produce a modular 2^l result where, "l" is less than "n"; and